

# Technology Risk Framework

## A Primer for Senior Bank Management

Henry J Becker

MIS Training Institute

The QB Group

7 Ashburn Place · Fair Lawn, NJ 07410

201 797-5901

[hbecker@misti.com](mailto:hbecker@misti.com)

[hbecker@qbgroup.com](mailto:hbecker@qbgroup.com)



THE  
QB  
GROUP

# Introduction (1/5)

---

As the senior executive of your bank you have always been challenged to provide your customers with services that are:

- What they want, and
- What they need

# Introduction (2/5)

---

*T*raditionally, before implementing any new service you and your managers analyze the business and regulatory issues and then make a decision to build or buy the system

# Introduction (3/5)

---

The analysis always included questions such as:

- ***Will the service...***
  - Attract new customers?
  - Help us keep existing customers?
- ***Is it...***
  - Competitive?
  - Cost effective?
- ***Will the regulators give us any trouble?***

# Introduction (4/5)

---

Once we decide to provide *any* form of computer-provided service (including service bureaus) we must also ask the question:

***Is the service and the data secure?***

- From employee, contractor and customer errors
- From employee, contractor and external hacking
- From failures and disasters
  - Network, hardware, physical

# Introduction (5/5)

---

In this session we will discuss how we discuss how a data processing manager or security manager performs a risk analysis of a financial data processing environment.

# Risk Assessment (1/4)

---

The risk assessment of a financial data processing environment includes:

- Transaction Analysis
  - Physical and manual processes
  - Electronic processes

# Risk Assessment (2/4)

---

The risk assessment of a financial data processing environment includes:

- Application program design
  - Data integrity
  - Error recovery
  - Audit and history logs
  - Application security
- Business Rules
  - Formulas
  - Procedures



# Risk Assessment (3/4)

---

The risk assessment of a financial data processing environment also includes:

- Open system interconnection (OSI) analysis which includes
  - The local area network (LAN)
  - The wide area network (WAN)
  - The computer operating system configurations (UNIX, NT, Netware)

# Risk Assessment (4/4)

---

The risk assessment of a financial data processing environment also includes:

- Disaster recovery and business contingency plans
  - Action plan
  - Real estate
  - Equipment
  - Networks
  - Staff

# In This Session

---

We will discuss some of the control strategies related to the security of electronic banking systems; specifically:

- Network security strategies
- Server and personal computer security strategies
- Password strategies
- Encryption strategies
- Wireless communication security

# Using Transaction Flow

---

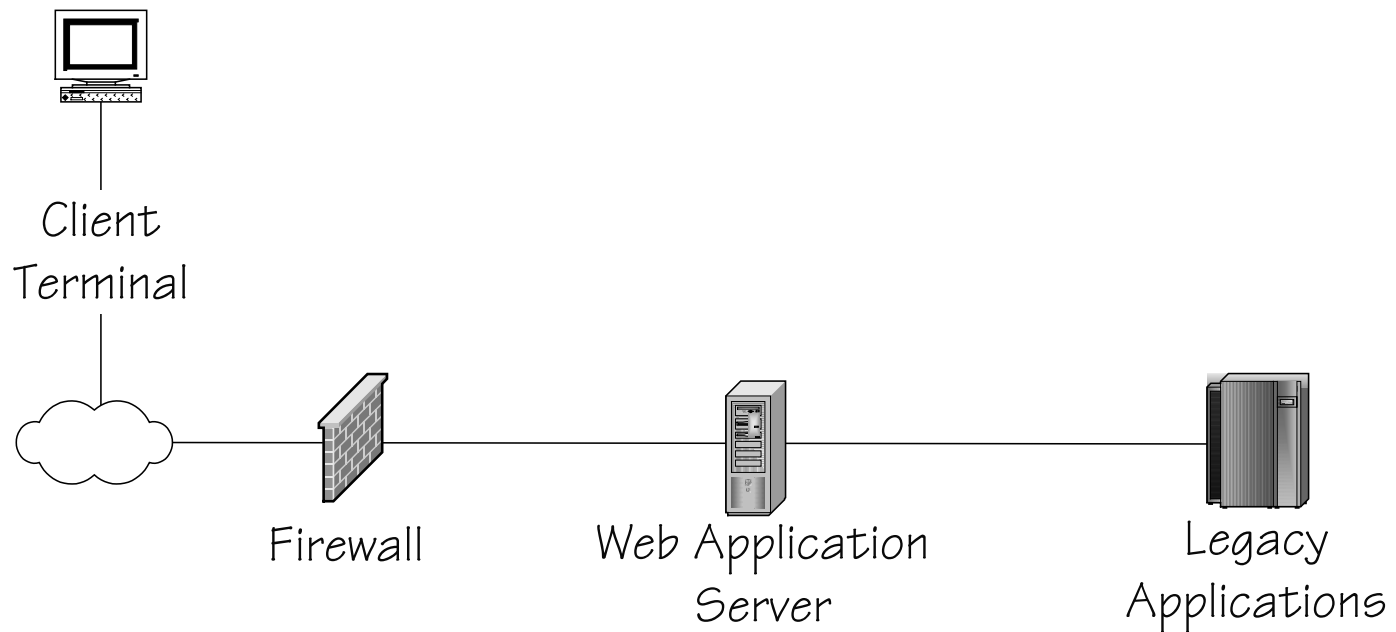
- Draw a picture of the path the transaction data follows – from client to server and back
- Label the work performed at each component
- Label the data that is sent between each component
- Perform a risk/exposure analysis of each component as it relates to the transaction and its data
- Apply appropriate controls

---

# Transaction Flow Analysis

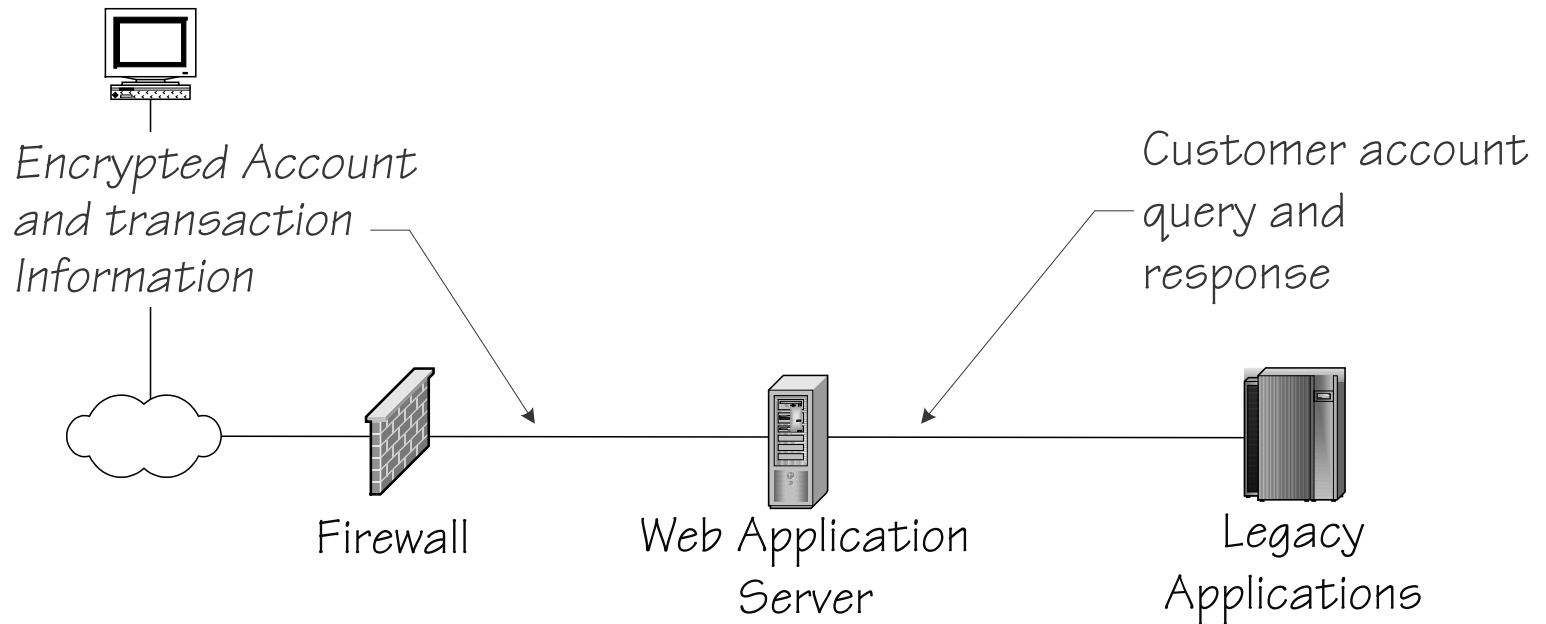
# Transaction Flow – In-house

---



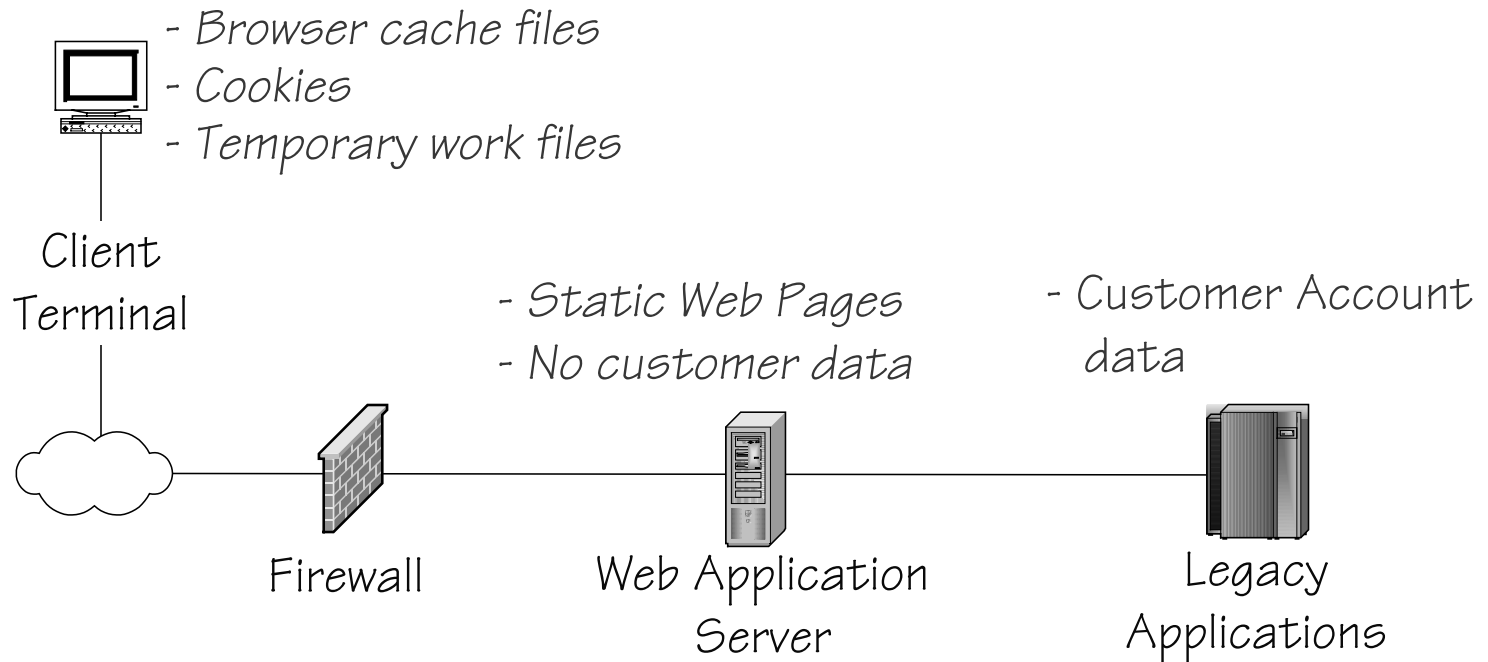
# Transaction Flow - Data Flow

---



# Transaction Flow – Application Location

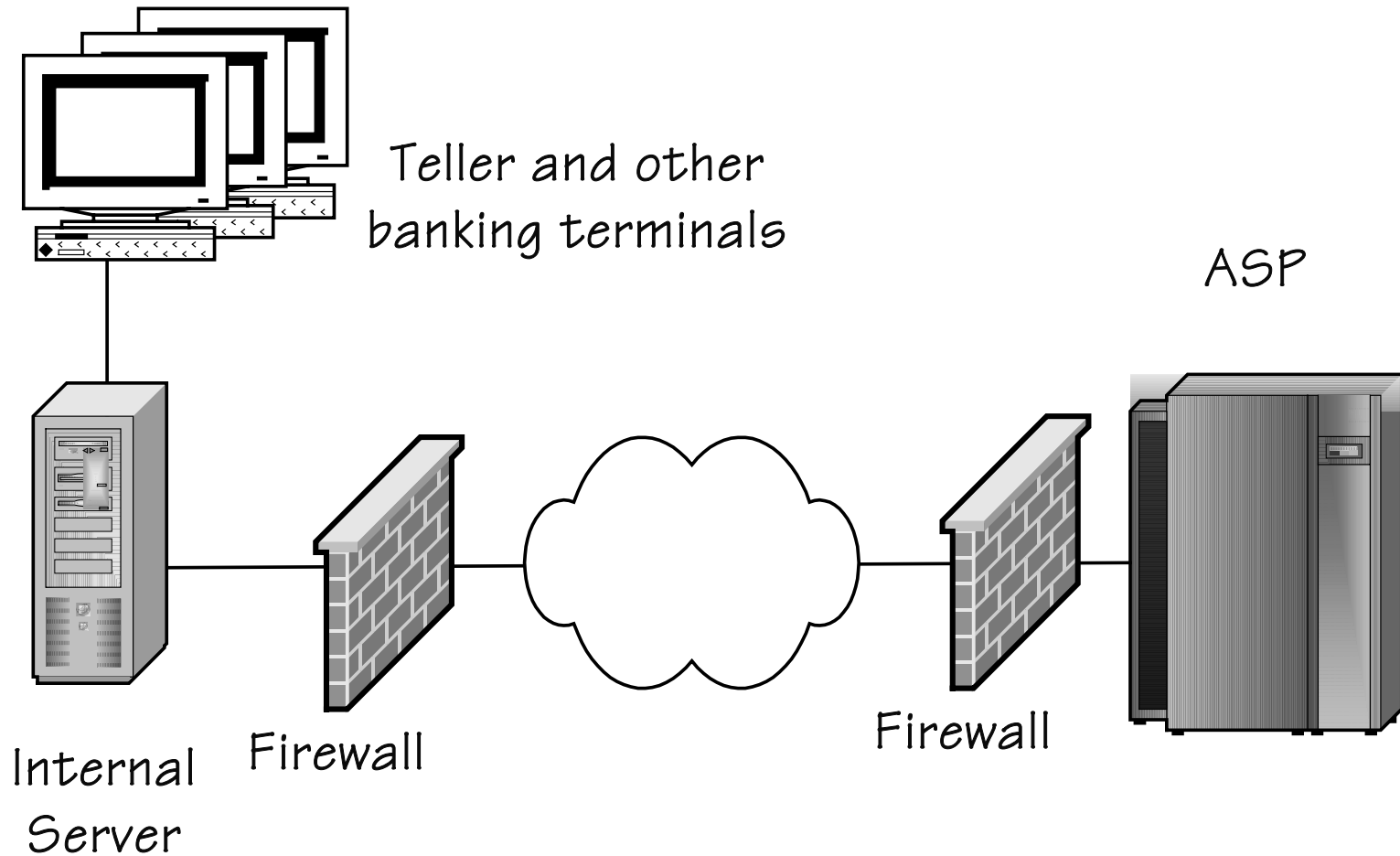
---





# Transaction Flow – Out Sourced

---



---

# Network Security Strategies

# Network Security Strategies

---

Network security means:

- Limiting access to all of the bank's terminals (usually personal computers) and servers from people and machines outside the bank
- Limiting access to sensitive terminals and servers from employees and contractors within the bank's four walls

This is properly done with **firewalls** and **routers**

# Network Reliability

---

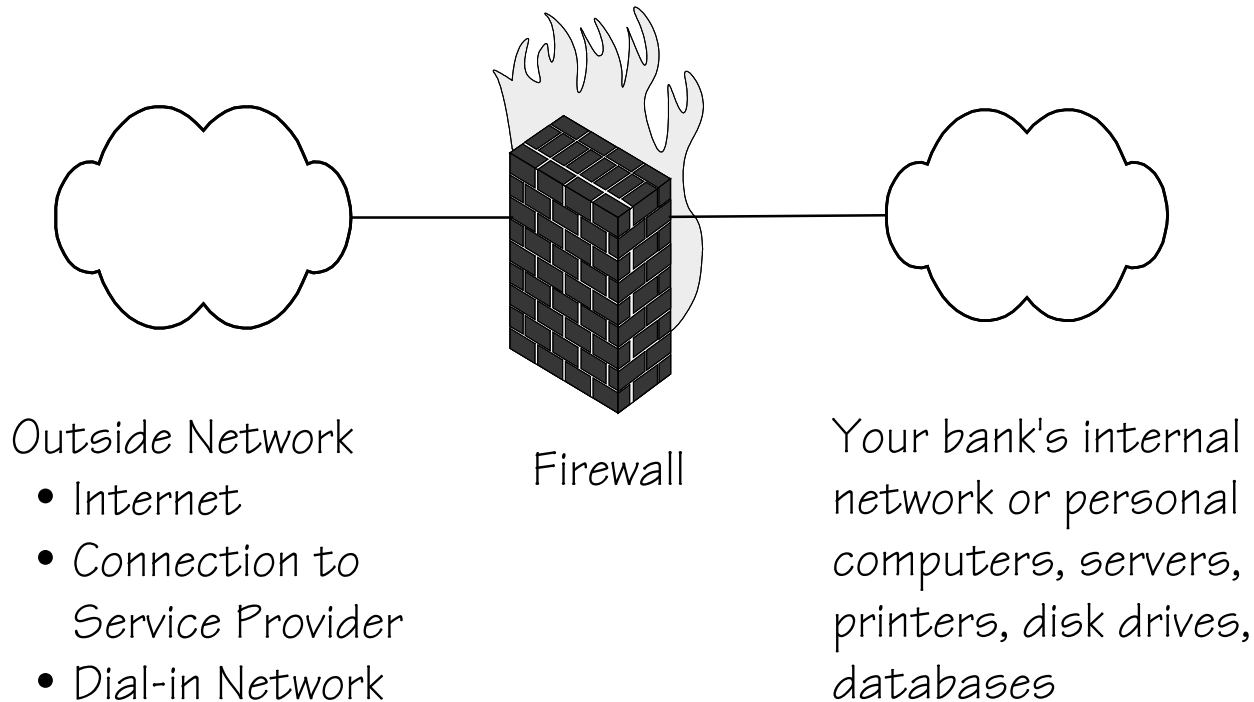
To ensure continuous connectivity:

- Ensure all network equipment is on uninterruptible power
- Consider connecting to more than one telephone company
- Ensure the cables exit two different points of the building and take totally different routes to the two phone companies
  - Physical diversity
  - Satellite for data

# Firewalls (1/4)

---

*A firewall is a piece of hardware or a program that runs on a dedicated computer. In a network diagram it is depicted like this:*



# Firewalls (2/4)

---

All data flowing through a network is generically called a message. Messages can be:

- Transactions that change data
  - Deposits, withdrawals, wire transfers, account posting
- Transactions that do not change data
  - Logins, database queries, electronic mail, web pages
- Messages are transmitted through the Internet and most corporate networks using the communication protocol called TCP/IP

# Firewalls (3/4)

---

Firewalls pass or block messages entering or leaving your bank's networks by inspecting every TCP/IP message passing through the firewall.

The inspection process is based on configuration rules that are set by your network manager, consultant or service provider.

# Firewalls (4/4)

---

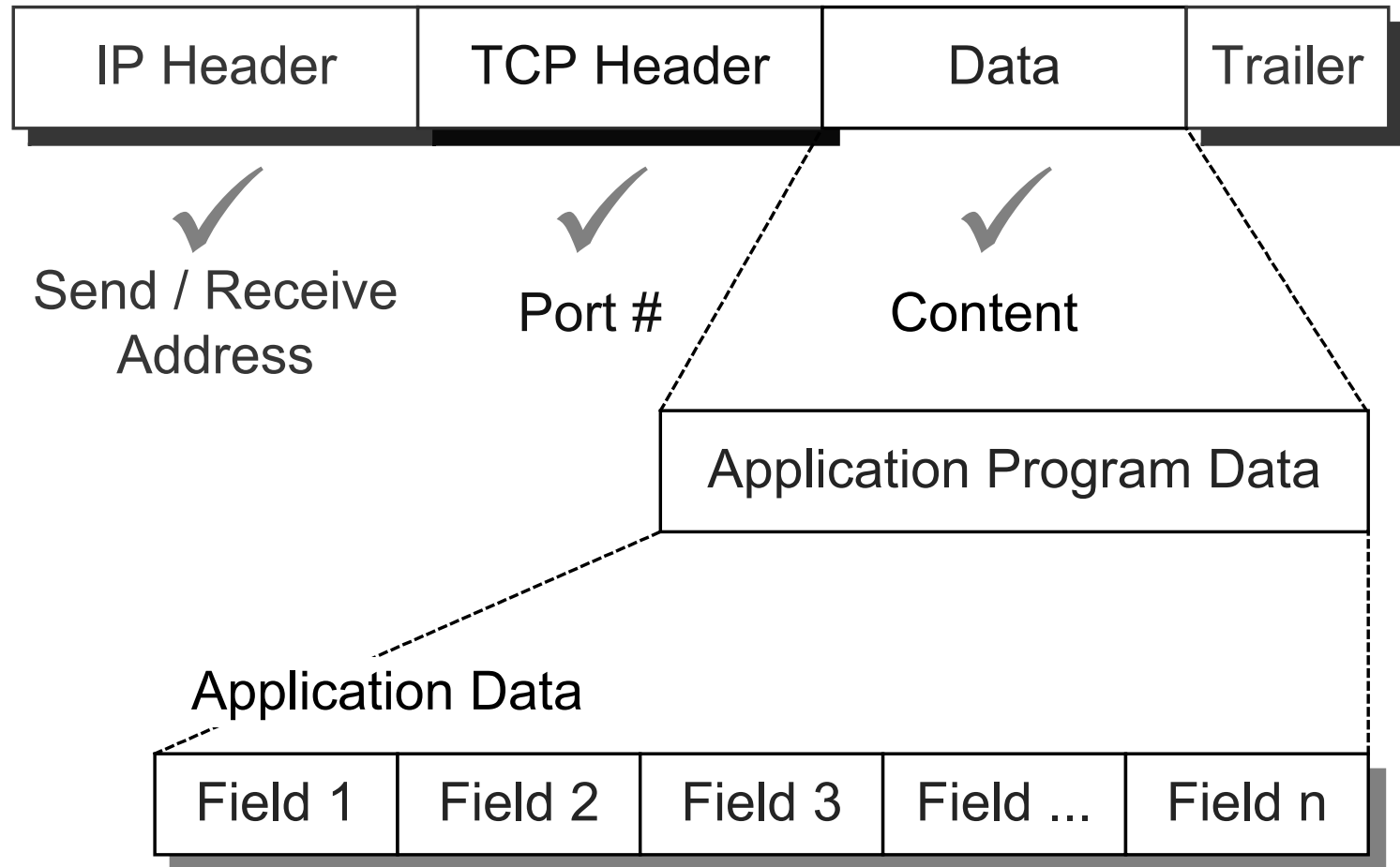
Configuration rules are the combination of testing one or more of the following five features of every message:

- The address of the sender and - or receiver
- The program originating and - or receiving the message
  - Every program on a networked computer has a numeric ID called a PORT number
- The data content within the message



# TCP/IP Message Format (1/2)

## TCP/IP Packet



# TCP/IP Message Format (2/2)

---

To: 192.168.13.5

From: 10.5.85.3

Originating Port#: 8325

Destination Port#: 8477

Data: Acct# 33498665

Transaction – e-payment

Payee: Offshore Acct B4XZ874

etc.....

# Firewalls

---









*Cisco PIX 501 Firewall*

# Sample Firewall Configuration

---

## Current Network Access Rules

#	Action	Service	Source	Destination	Time	Day	Enable		
1	Allow	IKE	*	192.168.168.168 (LAN)					
2	Deny	Default	*	LAN			<input checked="" type="checkbox"/>		
3	Allow	Default	LAN	*			<input checked="" type="checkbox"/>		

Add New Rule...

Restore Rules to Defaults

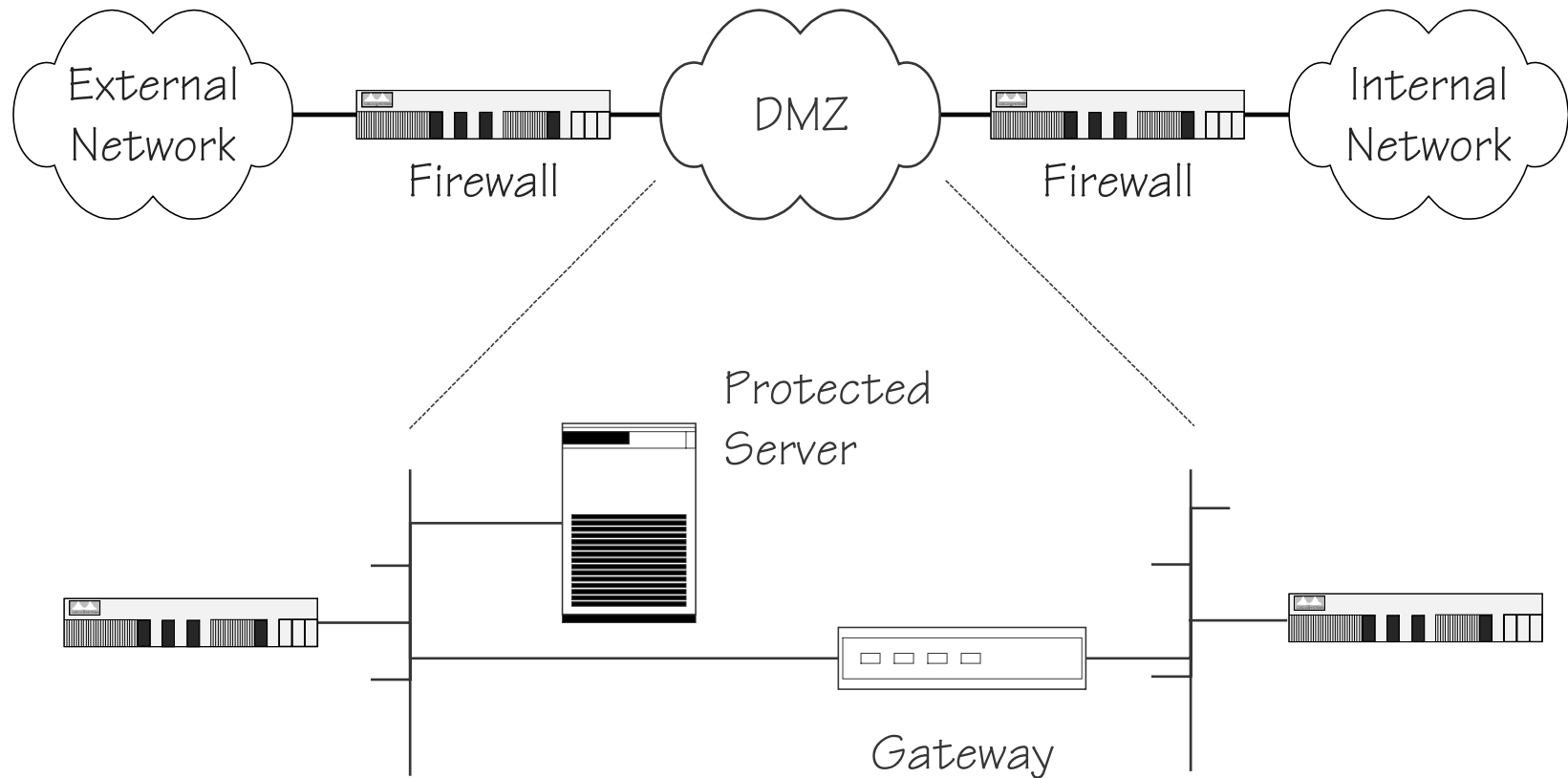


# The Demilitarized Zone (DMZ) (1/2)

---

- A common implementation of firewalls is to build a demilitarized zone that separates the servers to be protected from the outside and from the inside
- The dual-firewall configuration also makes it more difficult for a hacker to pass through both servers to get into the bank's network

# The Demilitarized Zone (DMZ) (2/2)



# Routers (1/3)

---

- Routers are used to move messages between different LANs
- Routers are also used to move messages between different physical locations that are connected with each other on the same network
  - Branches
  - Service providers

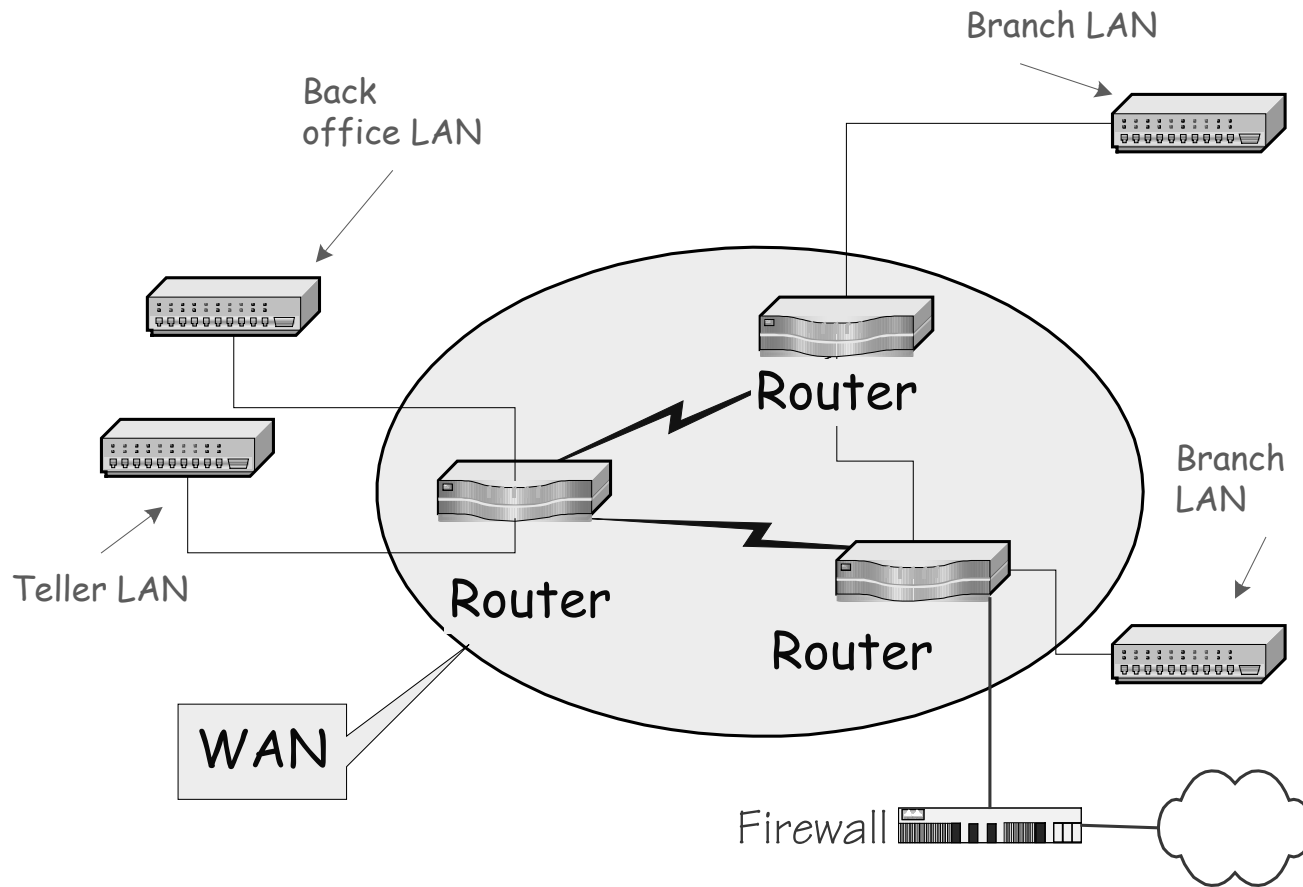
# Routers (2/3)

---

- Routers use the same rule strategy that is used by firewalls – with one exception; routers cannot check the data content within the message.
- Routers should not be used as firewalls
  - By default routers attempt to route all messages to the correct destination
  - By default firewalls will not pass any messages through the firewall



# Routers (3/3)



---

# Server and PC Security Strategies

# Server and PC Security Strategies (1/2)

---

To secure servers and personal computers you must:

- Apply security patches as soon as they become available
- Put each application on its own server
- Keep only the minimum number of support programs installed
- Remove all demo programs
- Limit access with firewalls, routers or stand-alone networks

# Server and PC Security Strategies (2/2)

---

- Use only the minimum number necessary user IDs
- Periodically evaluate the list of authorized users on each server
- Use all audit features
- Review audit records daily

---

# Authentication

# Authentication

---

Today, authentication is performed with:

- IDs and Passwords
- Biometrics
- Certificates
  - Public Key Infrastructure (PKI)

Other technologies such as voice and facial recognition are available but not very popular, reliable, or cost effective.

# Authentication: User IDs and Passwords (1/2)

---

The standard method of authenticating a user is via a user ID and password. Consider this:

- An employee or customer ID is usually predictable or publicly known
- *The password becomes the sole protection mechanism of the transaction and its data. To make this more threatening most systems require the password need only be entered once – at the beginning of the day !!!*
- The stronger the password - the more likely your data will remain secure

# Authentication: User IDs and Passwords (2/2)

---

Authentication based on passwords - *while not perfect* - can be made quite secure. For example:

- Make passwords eight characters or longer
- Require a mix of numbers and letters
- Do not allow words or acronyms
  - There are dictionary programs prevent this
- Change passwords every 30 – 45 days
- Lock out accounts with 2 or 3 unsuccessful attempts
- Investigate all lockouts not reported within one hour



# Authentication: Biometrics

---

Biometrics have become practical now that prices have become within reach of economic desktop deployment. Biometrics use one of the following characteristics of a person:

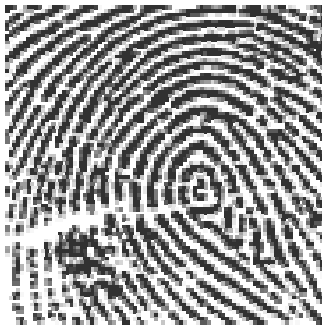
- Fingerprint
- Facial Recognition
- Iris pattern
- Retina pattern

# Authentication: Fingerprints (1/2)

---

## Fingerprint

- Converts the loops, arches and whorls of a fingerprint into a hash or message digest
  - A number that cannot be reversed back into the graphic of the fingerprint



Loops



Arches



Whorls

# Authentication: Fingerprints (2/2)

---



Courtesy Sony Corporation

# Authentication: Tokens (1/3)

---

- Tokens are handheld hardware devices that generate a pseudo-random (not predictable) 4, 6 or 8-digit number every minute
  - Each token has a unique algorithm – no two tokens generate the same sequence of minute-by-minute number
- Every protected host or system must have an authentication server
  - Users and their tokens are registered with the authentication server

# Authentication: Tokens (2/3)

---



Courtesy RSA Security Inc.

# Authentication: Tokens (3/3)

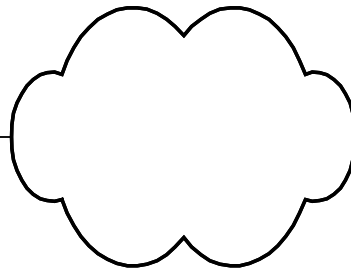
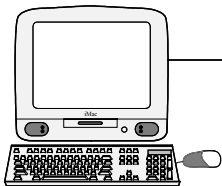
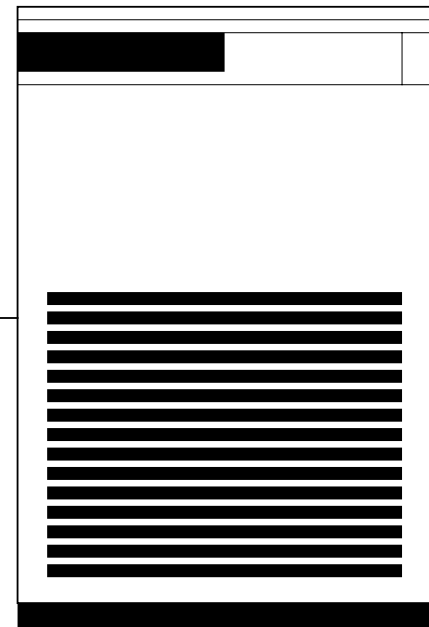
---

Customer, contractor  
and employee



User ID: Hank  
Password: \*\*\*\*\*  
SecurID: 332661

Server with  
authentication software



# Authentication: Smart Cards (1/3)

---

A smart card is a credit-card size piece of plastic that has:

- A microprocessor
- Some memory embedded in the upper left side of the card, and
- Electrical contacts to connect to the microprocessor

When the smart card is inserted in a reader attached to a point of sale, ATM, or personal computer, access to the microprocessor is enabled.

# Authentication: Smart Cards (2/3)

---

- The memory in the smart card can contain encryption keys, certificates, financial value, account numbers, etc.
- The contents of memory can be encrypted and decrypted by the embedded microprocessor.
- The encryption/decryption process can be activated by a PIN that is memorized by the owner of the smart card.



# Authentication: Smart Cards (3/3)

---



# Encryption Strategies

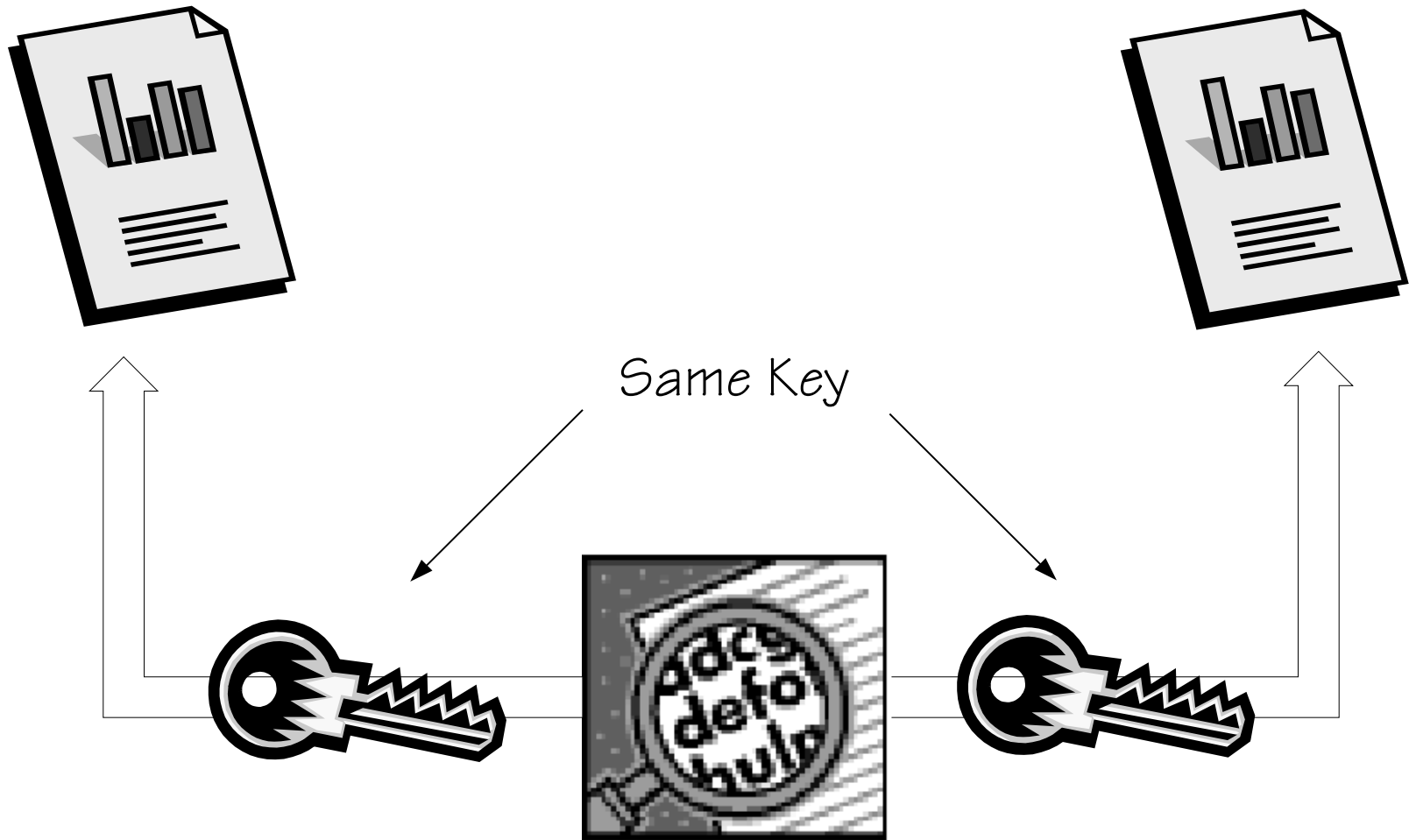
---

There are two types of encryption strategies

- Symmetric
  - All parties share the same password
  - AES (Rijndael), DES, triple-DES, Blowfish, IDEA, RC4, ...
- Asymmetric
  - Each participant has a pair of passwords
    - Diffie-Hellman, ElGamal,

# Symmetric Encryption

---



# Asymmetric Encryption

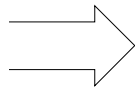


Asymmetric encryption means that one key encrypts a message (in this case the red key), and only the matching key (the green key) can decrypt the message.

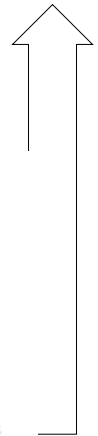
If the owner of the red key (called the private key), protects access to the key, then it can be assumed that only the holder of the red key could have encrypted and sent the message. This is the basis of trust and authentication.



Private Key



Public Key



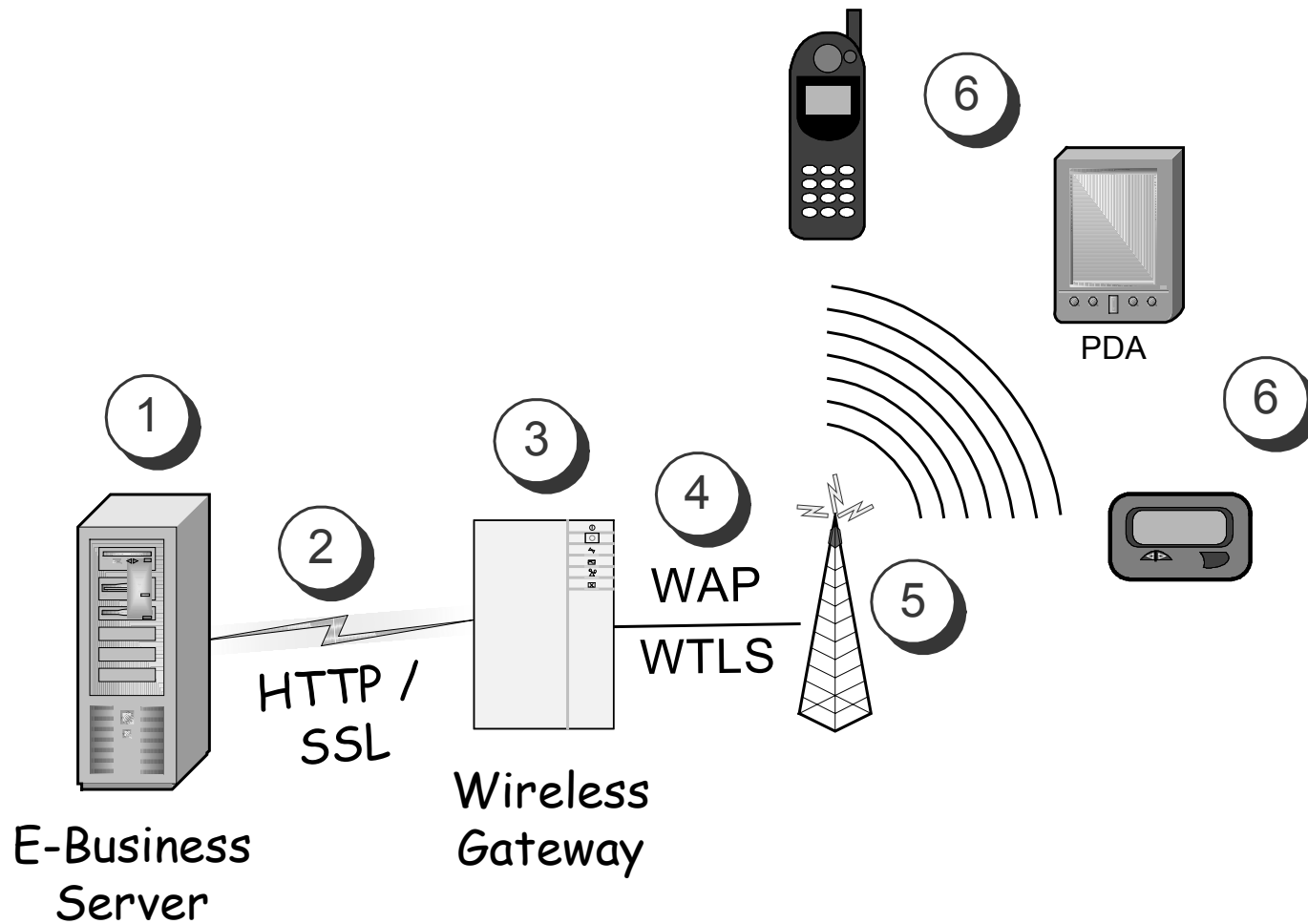
# Wireless Communication

---

Some banks and financial service providers are offering one-way and two-way wireless access via:

- One-way and two-way pagers
  - One-way alert messaging
- Cell phones with short message service (SMS)
  - One-way alert messaging
- Personal digital assistants and cell phones with browsers
  - Equivalent to *very slow* modem or Internet access

# Wireless Transaction Analysis (1/2)



# Wireless Transaction Analysis (2/2)

---

1. Secure application servers
2. Secure link between the server and the wireless gateway
3. Secure wireless gateway
4. Secure connection between the wireless gateway and the transmission system
5. Secure and reliable transmission system
6. Secure wireless devices

# Wireless LAN Communication

---

Additionally, some banks are considering or already have implemented wireless Ethernet local area networks to minimize the cost of installing new wiring or upgrading existing wiring.

The built-in security feature wired equivalency protocol (WEP) is *not secure*. To protect all data sent through a wireless LAN it must be encrypted by the application program or add-in product.



# Closing Comments (1/4)

---

Implementing a good security posture requires quality hardware and software support

- Firewalls
  - Not routers
- Intrusion detection
  - Identify anomalous activity
  - Intrusion detection software and audit trails
- Hardened servers
  - Dedicated to one function per server
  - Up-to-date security patches

# Closing Comments (2/4)

---

Implementing a good security posture requires risk avoiding procedures:

- Protected networks
- Protected servers and personal computers
- Reasonable authentication
  - Hard to guess passwords
  - Perhaps tokens or biometrics
- Secure encryption for public network and wireless communication

# Closing Comments (3/4)

---

Implementing a good security posture requires excellent manual practices

- Understanding the need for security
- Respect for security
- Training

# Closing Comments (4/4)

---

Minimizing risk also depends on:

- Developing and test a business recovery plan
- Verifying that *all* of the vendors you rely on also have business recovery plans

---

***Thank You***

# Vendor References

# Fingerprints

---

BioLink U-Match Mouse

- [www.biolinkusa.com](http://www.biolinkusa.com)

Compaq Fingerprint Technology

- [www.compaq.com](http://www.compaq.com)

DigitalPersona U.ar.U

- [www.digitalpersona.com](http://www.digitalpersona.com)

Ethentica Enhenticator

- [www.ethentica.com](http://www.ethentica.com)

Identix BioTouch

- [www.identix.com](http://www.identix.com)

SecurGen EyeD Hamster

- [www.securgen.com](http://www.securgen.com)

Sony FIU-710

- [www.cony.co.jp/en/Products/puppy](http://www.cony.co.jp/en/Products/puppy)

# Firewall Vendors

---

## Hardware

- Axent
- Cisco
- Cyberguard
- Network-1
- Nokia
- Nortel
- Sonic Systems
- WatchGuard Technologies

## Software

- Checkpoint Software Technologies
- Network-1
- Network Associates
- Network Ice
- Symantec



# Smart Cards

---

Gemplus

- [www.gemplus.com](http://www.gemplus.com)

Visa (Smart Debit, Smart Credit)

- [www.visa.com](http://www.visa.com)

Smart Card Industry Association (SCIA)

- [www.scia.org](http://www.scia.org)

American Express (Blue)

[www.americanexpress.com](http://www.americanexpress.com)

# Tokens

---

Aladdin Knowledge Systems

- [www.eladdin.com](http://www.eladdin.com)

RSA Security Inc

- [www.rsa.com](http://www.rsa.com)

Vasco

- [www.vasco.com](http://www.vasco.com)